Pakistan Journal of Positive Psychology

Print ISSN : 3078-6428 | Online ISSN : 3078-6436
Pakistan Journal of Positive Psychology

Original Article

FROM OWNERSHIP TO ACTION: THE ROLE OF SPIRAL OF SILENCE IN INFORMATION SECURITY BEHAVIOR

Gulyana Shehzad [a*], Dr. Aisha Zubair [b], Muhammad Usman [c], & Faheem Shehzad [d]

[a] PhD Scholar, National Institute of Psychology, Quaid-i-Azam University, Islamabad, Pakistan. Email: gulyanashehzad@yahoo.com
[b] Assistant Professor, National Institute of Psychology, Quaid-i-Azam University, Islamabad, Pakistan. Email: aishazubair@nip.edu.pk
[c] MPhil, National Institute of Psychology, Quaid-i-Azam University, Islamabad, Pakistan. Email: usmanqau7@gmail.com
[d] MS Information Security, National University of Science and Technology, Islamabad, Pakistan. Email: faheemshehzad7@gmail.com

*Correspondence to: Mr. Gulyana Shehzad, PhD Scholar, National Institute of Psychology, Quaid-i-Azam University, Islamabad, Pakistan. Email: gulyanashehzad@yahoo.com

KEYWORDS:
Psychological Ownership, Spiral of Silence, Information Security Behavior, Cybersecurity, Employee Silence

CITE THIS ARTICLE:
Shehzad, G., Zubair, A., Usman, M., & Shehzad, F. (2026). From ownership to action: the role of spiral of silence in information security behavior. Pakistan Journal of Positive Psychology, 3(9), 176-185.

ABSTRACT

Drawing on psychological ownership and spiral-of-silence perspectives, this study examined the relationships among psychological ownership, spiral of silence, and information security behavior, with particular attention to the mediating role of employee silence. Using a cross-sectional survey design, data were collected from 550 employees. Psychological ownership was assessed using the Psychological Ownership Questionnaire (Avey et al., 2009), spiral of silence through the Spiral of Silence Scale (Lee et al., 2014), and information security behavior using the Security Behavior Intentions Scale (SeBIS; Egelman & Peer, 2015). The findings revealed that greater psychological ownership was associated with stronger information security behavior and lower levels of spiral of silence. Employees reporting greater reluctance to express cybersecurity-related concerns also tended to report weaker information security behavior. Furthermore, the findings supported an indirect pathway in which psychological ownership was associated with stronger information security behavior partly through reduced spiral of silence, while a substantial direct relationship between psychological ownership and security behavior remained. Moreover, in demographics, women reported greater psychological ownership, silence, and security behavior than men. Certified employees reported greater ownership and less silence. These findings extend behavioral cybersecurity research by demonstrating that secure workplace behavior involves not only individual responsibility but also the social conditions surrounding cybersecurity communication. Employees who develop a stronger sense of ownership toward organizational resources may be more inclined to protect those resources and less likely to remain silent about potential security concerns. Organizations should therefore complement technical safeguards and conventional cybersecurity training with practices that strengthen employee responsibility and create psychologically safe, accessible, and nonpunitive opportunities for communicating vulnerabilities, mistakes, and unsafe practices. Given the cross-sectional and self-report design, longitudinal and behavioral research is needed to establish the temporal direction of these relationships.

I. INTRODUCTION

Organizational information security depends on decisions made throughout the working day. Employees choose how to handle sensitive information, protect devices, respond to unfamiliar requests, and maintain secure access

to digital resources. Technical safeguards provide essential protection, but their effectiveness also depends on how people use systems and respond when something appears unsafe. Behavioral cybersecurity research has consequently examined why employees comply with security requirements and why protective conduct varies across individuals and workplaces. Cram et al. (2019), in a meta-analysis of information security policy compliance, identified a substantial body of evidence involving multiple individual and organizational antecedents. Their synthesis supports an approach that considers employees' motivations and working conditions alongside formal controls. A further organizational challenge concerns information that employees possess but do not communicate. Someone may follow recommended password practices while avoiding a conversation about an unsafe procedure. An employee may also notice a questionable request but hesitate to challenge the colleague or supervisor responsible for it. These examples illustrate a conceptual distinction between maintaining secure personal practices and expressing security-related concerns. Research on employee voice and silence emphasizes that useful information does not automatically reach organizational decision makers simply because employees have opportunities to speak (Morrison, 2023). Understanding information security therefore requires attention to both employees' relationship with organizational resources and the social pressures surrounding communication. The present study brings these issues together by examining psychological ownership, spiral of silence, and information security behavior. Psychological ownership concerns the felt possession of a target; spiral of silence concerns reluctance to express opinions when perceived social support is weak; and information security behavior concerns protective practices. The proposed model treats ownership as the predictor, silence as a potential explanatory pathway, and security behavior as the outcome. Its central question is whether employees who experience stronger ownership also report less silence and more secure practices, and whether the ownership–behavior relationship includes an indirect association through silence.

Psychological Ownership and Protective Responsibility

Psychological ownership describes the experience that an organization, role, project, or other target belongs to oneself, even when legal ownership is absent. Pierce et al. (2001) identified perceived control, intimate knowledge, and investment of the self as important routes through which this experience develops. These routes are relevant to organizational information systems: employees can contribute to a system's operation, acquire detailed knowledge of its functions, and invest considerable effort in maintaining it. Such involvement may make the target personally meaningful. Psychological ownership is therefore distinguishable from assigned responsibility, because holding a formal role does not necessarily imply feeling personally connected to the resources involved. Organizational research provides a basis for expecting ownership to relate to constructive conduct. Van Dyne and Pierce (2004) examined psychological ownership in three field studies and linked it with employee attitudes and organizational citizenship behavior. Avey et al. (2009) further distinguished promotion-focused ownership, involving self-efficacy, accountability, belongingness, and self-identity, from territoriality. Together, these perspectives suggest that felt possession can accompany investment in organizational welfare, although different forms of ownership need not produce the same outcomes. In the present model, the relevant rationale concerns constructive ownership and the responsibility employees may experience toward valued organizational resources. The application to information security is plausible but requires empirical testing. An employee who feels connected to organizational resources may regard their protection as personally important and may be more willing to sustain protective effort. Verkijika (2020) provided security-specific evidence by examining psychological ownership as a boundary condition in the relationship between security self-efficacy and mobile security behavior. That study suggests ownership can help explain when confidence is associated with protective action. It does not, however, establish the communication pathway proposed here. The present study extends this reasoning by considering whether ownership is associated with the withholding of security-related opinions as well as reported security practices.

Spiral of Silence in Organizational Cybersecurity

Spiral-of-silence theory explains how perceived opinion climates can influence public expression. Individuals assess whether their views appear socially supported and may withhold them when expression is expected to invite isolation or disapproval (Noelle-Neumann, 1974). As dissenting views become less visible, an apparent consensus can strengthen, potentially discouraging further expression. Bowen and Blackmon (2003) brought this perspective into organizational voice research, highlighting how social isolation can restrict employees' willingness to speak. Applied to cybersecurity, the theory suggests that employees' private assessments of risk may differ from the

opinions they are prepared to express to others. Security concerns can be socially inconvenient. Questioning an established procedure may challenge a colleague's judgment, reveal one's own uncertainty, or conflict with a manager's preferred course of action. An employee who believes that others dismiss security concerns may decide that expressing a different view would damage workplace relationships. This proposed mechanism differs from simply lacking knowledge or having nothing useful to report. It also differs from silence motivated entirely by futility or confidentiality. Morrison (2023) reviews the broader complexity of employee silence; the spiral-of-silence perspective focuses more specifically on perceived social support and anticipated isolation. Recent research demonstrates that this perspective already has a place in information security scholarship. Petrič and Orehek (2025) examined employees' willingness to express organizational security opinions to coworkers and management. Their survey findings indicated that employees with positive security opinions could remain silent when they perceived those opinions as unsupported by coworkers. This evidence highlights the possibility of a discrepancy between private security judgments and visible workplace opinion. More recently, Marett and Marett (2026) used an experimental vignette design to examine safety voice and managerial intentions concerning information security. These studies establish the relevance of communication while leaving room to investigate its connection with felt ownership and personal protective practices.

Relationship Among Ownership, Silence, and Security Behavior

Psychological ownership offers a possible explanation for variation in silence because felt possession may influence how employees evaluate the consequences of withholding a concern. When organizational resources matter personally, remaining silent about a perceived weakness may conflict with a sense of responsibility. Employees may also feel greater legitimacy to raise questions about resources in which they have invested effort. This argument combines the stewardship implications of ownership theory with the social inhibition described by spiral-of-silence theory. It yields the expectation that stronger psychological ownership will be associated with less silence, while recognizing that this relationship is a proposed extension rather than an established consequence of ownership. There are reasons to avoid assuming that ownership invariably encourages expression. An employee may feel strongly attached to a system yet conceal a problem to protect their reputation or retain control. Avey et al.'s (2009) distinction between constructive ownership and territoriality is relevant to this possibility. Likewise, valuing a resource does not remove the interpersonal costs of questioning an influential colleague. The present hypothesis therefore concerns an expected average association, rather than a claim that ownership overrides every social barrier. A finding inconsistent with that expectation would be theoretically informative, particularly if the measured ownership construct includes defensive or territorial elements. Silence may also be associated with weaker security practices through reduced opportunities for clarification and corrective feedback. Discussing a questionable request can help an employee decide how to respond; asking about a difficult procedure can reveal a safer alternative. When such communication is withheld, uncertainty or problematic routines may remain unresolved. This is the proposed link between silence and the behavioral outcome. Nevertheless, communication and personal security practices should remain conceptually distinct: low silence does not necessarily imply strong password habits, and careful device protection does not establish willingness to raise concerns. The model tests their association without defining either construct as the reverse of the other.

This distinction is particularly important for the study's operationalization of information security behavior. The Security Behavior Intentions Scale developed by Egelman and Peer (2015) covers password practices, device securement, updating, and proactive awareness. It captures respondents' reported tendencies concerning recommended security practices rather than a comprehensive record of workplace security performance. Consequently, the present outcome should be understood as self-reported security behavior and intentions. The theoretical relevance of incident reporting and constructive challenge does not imply that the behavioral outcome directly measures those activities. The study instead examines whether reluctance to express security opinions is associated with the personal security practices represented by the instrument. Ownership research explains why organizational resources may become personally significant, whereas spiral-of-silence research explains why relevant opinions may remain unexpressed. Existing studies already connect ownership with cybersecurity and examine opinion expression in security settings. The contribution proposed here is therefore a focused examination of whether silence helps account for the ownership–behavior association. By linking felt possession with the social inhibition of expression, the model examines a communication-based explanation alongside the direct association between ownership and protective conduct.

The study examines the direct relationships among the three constructs and the proposed indirect association from ownership to security behavior through silence. Ownership may be associated with protective practices independently of communication, while reduced silence may represent an additional pathway. Because the design is cross-sectional, this ordering expresses a theoretical expectation rather than demonstrated temporal sequence. Secure practices could strengthen ownership, and unmeasured organizational conditions could influence all three constructs. On this basis, the following hypotheses are proposed:

H1. Psychological ownership will positively predict information security behavior.
H2. Psychological ownership will negatively predict spiral of silence.
H3. Spiral of silence is negatively associated with information security behavior.
H4. Spiral of silence mediates the relationship between psychological and information security behavior.

II. METHOD

Participants

The study employed a cross-sectional, non-experimental survey design to examine relationships among psychological ownership, spiral of silence, and self-reported information security behavior. Psychological ownership was specified as the predictor, spiral of silence as the proposed intervening variable, and information security behavior as the outcome. The design permits examination of concurrent associations and a theoretically specified indirect association. Cross-sectional indirect effects can differ substantially from longitudinal mediation processes (Maxwell & Cole, 2007). The current study consists of 550 employees. Of these, 358 were men and 192 were women; 280 were graduates and 270 were postgraduates. In this study 352 had received cybersecurity training, 383 held a cybersecurity certification, 310 worked onsite, and 240 worked in hybrid arrangements.

Measures

Psychological Ownership Questionnaire. The Psychological Ownership Questionnaire (POQ), developed by Avey et al. (2009), is a self-report instrument designed to assess employees' psychological ownership within organizations. It consists of 16 items covering five dimensions. Self-efficacy (3 items) assesses confidence in contributing to organizational success. Accountability (3 items) assesses willingness to hold oneself and others accountable for organizational practices. Belongingness (3 items) measures feelings of belonging and comfort within the organization. Self-identity (3 items) assesses the extent to which organizational membership and success form part of an individual's identity. These four dimensions constitute promotion-focused psychological ownership. Territoriality (4 items) measures a protective or defensive orientation toward ideas, workspace, and other ownership targets and represents prevention-focused ownership. Responses are recorded on a six-point Likert-type scale, ranging from 1 (strongly disagree) to 6 (strongly agree). Avey et al. reported Cronbach's alpha coefficients of .90, .81, .92, .73, and .84 for self-efficacy, accountability, belongingness, self-identity, and territoriality, respectively, in their initial sample. Their subsequent sample yielded $\alpha = .91$ for overall promotion-focused ownership. Territoriality should be scored separately from the 12 promotion-focused items.

Spiral of Silence Scale. The spiral-of-silence measures associated with Lee et al. (2014) assess individuals' responses to expressing opinions in potentially unfavorable social situations. The seven-item version documented by Bayram and Bayer (2019) contains three components. Opinion-expression avoidance (2 items) concerns concealing one's position through apparent agreement or neutral comments. Opinion-expression engagement (2 items) concerns openly discussing or stating one's own views. Fear of isolation (3 items) assesses concerns about exclusion or unfavorable interpersonal reactions when others disagree. Responses are recorded on a five-point Likert-type scale, ranging from 1 (strongly disagree) to 5 (strongly agree). In the Turkish adaptation, Cronbach's alpha coefficients were .654 for the avoidance-related items, .635 for engagement, and .877 for fear of isolation; the overall coefficient was .641. Because engagement represents greater expression rather than greater silence, the scoring direction must be checked before calculating an overall silence score. The measure should be described as assessing cybersecurity-related silence only when the administered items explicitly address workplace security concerns.

Information Security Behavior Intentions Scale. The Security Behavior Intentions Scale (SeBIS), developed by Egelman and Peer (2015), is a self-report instrument designed to assess adherence to computer-security practices. It consists of 16 items distributed across four subscales. Device securement (4 items) assesses practices such as locking computers and using passwords or passcodes to protect devices. Password generation (4 items) assesses password creation and management practices. Proactive awareness (5 items) evaluates attention to potential security risks, including checking links and website security. Updating (3 items) assesses practices related to installing software updates and maintaining updated programs. Responses use a five-point frequency scale: 1 (never), 2 (rarely), 3 (sometimes), 4 (often), and 5 (always). Negatively keyed items are reverse-scored so that higher scores indicate greater adherence to security practices. An unweighted total ranges from 16 to 80, while an item-average score ranges from 1 to 5. The original development study reported overall Cronbach's $\alpha = .801$, with coefficients of .728 for device securement, .764 for password generation, .668 for proactive awareness, and .719 for updating.

Procedure

Data was collected using a structured, self-administered questionnaire distributed to eligible employees in the participating organizations. Before data collection, permission was obtained from the relevant organizational authorities. Potential participants were informed about the study's purpose and screened against the inclusion and exclusion criteria. Eligible employees who voluntarily agreed to participate received an information sheet describing the study objectives, procedures, anticipated benefits, and potential risks. Informed consent was obtained before participants completed the questionnaire. The questionnaire included demographic questions and measures of psychological ownership, spiral of silence, and information security behavior. Participants received standardized instructions and were asked to respond independently, drawing on their workplace experiences and usual security practices. The researcher remained available to clarify instructions without influencing responses. Participants were encouraged to answer honestly and were assured that their individual responses would not be shared with supervisors or used to evaluate their job performance. Participation was voluntary, and employees could decline participation or discontinue the questionnaire without penalty. No personally identifiable information was recorded on the questionnaires, and responses were treated confidentially. Participants were instructed to avoid disclosing passwords, confidential organizational information, or identifiable details about security incidents. Completed questionnaires were reviewed for missing responses, and missing data were handled according to the study's specified criteria. Data were stored securely, accessed only by the research team, and used solely for academic purposes. Findings were reported in aggregate form to protect participants' privacy.

III. RESULTS

Correlations

Psychological ownership was strongly and negatively correlated with spiral of silence ($r = -.76$, $p < .001$) and strongly and positively correlated with self-reported security behavior ($r = .70$, $p < .001$). Thus, employees with greater psychological ownership reported less silence and stronger security practices. Spiral of silence was also strongly and negatively correlated with self-reported security behavior ($r = -.72$, $p < .001$), indicating that greater reluctance to express opinions was associated with weaker reported security practices.

Hierarchical Regression

Table 1 presents the hierarchical regression results for information security behavior. In the first model, greater psychological ownership was associated with stronger reported security practices. Adding spiral of silence improved the model's explanatory power. Psychological ownership remained positively associated with security behavior, while greater silence was associated with poorer reported security practices after accounting for ownership. These findings suggest that psychological ownership and spiral of silence each contribute to explaining differences in employees' reported security behavior.

Table I: Hierarchical Regression Predicting Security Behavior

Predictors	Model 1 β	95% CI LL	95% CI UL	Model 2 β	95% CI LL	95% CI UL
Psychological ownership	.60**	.53	.66	.45**	.38	.52
Spiral of silence	-	-	-	-.30**	-.38	-.23
R^2	.36			.43		
Adjusted R^2	.35			.43		
ΔR^2	.36			.07		
F	308.25**			211.01**		
ΔF	308.25**			73.18**		

**$p < .001$

Mediation Analysis

Greater psychological ownership was associated with less spiral of silence, while greater silence was associated with poorer reported security behavior after accounting for ownership. Psychological ownership also remained positively associated with security behavior after accounting for silence. Together, these relationships suggest that reduced silence may partly explain the positive association between ownership and security behavior. The pattern is consistent with the proposed partial mediation model, but confirmation requires a verified indirect-effect analysis.

Table II: Standardized Mediation Estimates for Psychological Ownership, Spiral of Silence, and Information Security Behavior

Path or effect	Path	β	SE	95% CI
Psychological ownership → Spiral of silence	a	-.760	.028	[−.815, −.705]
Spiral of silence → Security behavior, controlling for ownership	b	-.445	.043	[−.529, −.361]
Direct ownership → Security behavior association, controlling for silence	c′	.362	.043	[.277, .446]
Indirect association through spiral of silence	ab	.338	--	--
Total ownership → Security behavior association	c	.700	.031	[.640, .760]

Group Differences

Women reported greater psychological ownership than men, indicating a stronger sense of personal connection, belonging, and identification with their organization. This was the most pronounced gender difference among the study variables. Women also reported higher spiral-of-silence scores, suggesting greater reluctance to express their opinions or greater concern about unfavorable social reactions. At the same time, women reported stronger information security behavior, reflecting greater adherence to the protective practices assessed by the security measure. The differences in silence and security behavior were broadly comparable in magnitude. Taken together, the pattern indicates that stronger organizational attachment and more secure personal practices can coexist with greater hesitation about expressing opinions.

Table III: Independent-Samples t Tests for Gender Differences Across Study Variables (N = 550; Men: n = 358; women: n = 192)

	Men		Women				
Variables	*M*	*SD*	*M*	*SD*	*t*(548)	*p*	Cohen's *d*
Psychological Ownership	32.25	8.32	37.78	7.43	-5.64	.00	.73
Spiral of Silence	23.5	5.77	26.7	5.66	3.88	.01	.46
Information Security Behavior	54.22	7.55	57.88	4.33	4.77	.00	.51

Table 3 shows that employees with cybersecurity certification reported greater psychological ownership than those without certification, indicating stronger organizational attachment and identification. Certified employees also reported less spiral of silence, suggesting lower reluctance to express their views in potentially unfavorable social situations. Their reported information security behavior was higher as well, reflecting a more favorable pattern of protective practices, subject to confirmation of the security-score calculation. The largest standardized difference concerned security behavior, followed by silence, while the ownership difference was comparatively

smaller. Overall, the supplied group means show a consistent pattern of greater ownership, lower silence, and stronger reported security practices among certified employees.

Table IV: Cybersecurity Certifications Received Differences Across Study Variables (N = 550; Yes: n = 383; no: n = 167)

	Yes		No				
Variables	*M*	*SD*	*M*	*SD*	*t*(548)	*p*	Cohen's *d*
Psychological Ownership	36.25	8.32	32.78	7.43	4.64	.00	.38
Spiral of Silence	23.50	5.77	26.70	5.66	3.88	.01	.46
Information Security Behavior	88.22	7.55	83.88	5.33	6.77	.00	.61

IV.DISCUSSION

The study examined whether ownership and silence provide complementary explanations of self-reported information security behavior. The results show a positive ownership–behavior association that remains after accounting for silence. This is consistent with psychological ownership theory, which links felt possession to personal investment in a valued target (Pierce et al., 2001). Employees who experience organizational resources as personally meaningful may devote greater attention and effort to their protection. The findings also fit broader organizational evidence connecting ownership with citizenship-related conduct (Van Dyne & Pierce, 2004). In cybersecurity, Verkijika (2020) found that ownership helped explain variation in the relationship between security self-efficacy and mobile security behavior. The present model addresses a different question by considering silence as a possible intervening association. Its contribution is therefore the integration of felt possession and communication reluctance, rather than a claim that ownership has not previously been studied in security settings. Comparisons remain qualified because instrument targets and behavioral domains may differ across studies. Ownership should not be equated with formal accountability or treated as uniformly beneficial. Avey et al. (2009) distinguish constructive ownership from territoriality, suggesting that felt possession can accompany either engagement or defensive control. If the administered questionnaire combines those forms, the observed relationship may be difficult to interpret. Confirming the ownership score is therefore central to the theoretical contribution. Without security-specific item wording, the results concern general organizational ownership rather than ownership of information assets specifically.

The negative silence-behavior association suggests that communication reluctance may accompany weaker personal security practices. A possible explanation is that employees who avoid expressing concerns obtain less clarification or corrective feedback about uncertain situations. However, this explanation remains theoretical: the survey summaries do not show that silence delayed reporting, prevented feedback, or caused a security incident. A broader workplace climate could also influence both communication and protective habits. The finding is consistent with the relevance of opinion climate established by Petrič and Orehek (2025), who examined security opinion expression among employees. It also connects with the wider distinction between employee voice and silence reviewed by Morrison (2023). Silence can reflect several motives, and fear of isolation is only one possible explanation. Because the source instrument originated in public-opinion research, its adaptation must demonstrate that the score used here actually captures the proposed workplace mechanism. General reluctance to express opinions should not automatically be interpreted as deliberate withholding of cybersecurity concerns.
Importantly, the outcome does not measure security voice. SeBIS assesses reported practices concerning devices, passwords, updating, and proactive awareness (Egelman & Peer, 2015). The present association therefore links a communication-related construct with personal protective tendencies rather than showing that employees who speak up report more incidents. Recent experimental work by Marett and Marett (2026) addresses managerial responses to safety voice in security settings, illustrating a related but distinct outcome. These distinctions prevent the focused model from overstating what its measures can establish.

The positive product of the ownership-to-silence and silence-to-behavior associations is consistent with the proposed explanation that stronger ownership accompanies less silence, which in turn accompanies more secure reported practices. The remaining ownership coefficient suggests that communication reluctance would not

account for the entire ownership–behavior association. Nevertheless, an indirect-effect estimate alone is insufficient to establish statistical mediation, especially while its uncertainty and scoring remain unverified. The group comparisons suggest that gender and cybersecurity certification may be relevant to understanding variation in the study variables. Women reported greater psychological ownership and stronger security practices alongside higher silence. This combination indicates that personal protective behavior and reluctance to express opinions can coexist. It does not contradict the negative individual-level association between silence and security behavior, because group mean differences and associations across individuals address different questions. Certified employees reported greater ownership, less silence, and higher security-behavior scores. Professional preparation or greater familiarity with security responsibilities could help explain this pattern, although occupational role, prior experience, organizational support, and selection into certification provide alternative explanations.

The cross-sectional design also leaves alternative sequences open. Secure habits may strengthen ownership by increasing familiarity and investment, while supportive management may simultaneously encourage ownership, reduce silence, and improve security practices. Maxwell and Cole (2007) show why cross-sectional decompositions can misrepresent longitudinal mediation. Accordingly, the present estimate should be treated as a provisional associational pattern. A longitudinal design measuring ownership, subsequent silence, and later behavior would provide a more informative test, although temporal separation alone would not eliminate confounding. The two-variable predictor model accounts for approximately 43.6% of outcome variance in the supplied matrix, with silence adding information beyond ownership alone. This result indicates a potentially useful combined model, but explained variance is not evidence that an intervention will produce an equivalent improvement in security. The original study included awareness, and the present reanalysis cannot show that the focused relationships are independent of awareness or other omitted influences.

Limitations

First, the cross-sectional design does not establish temporal order or causation. The indirect point estimate represents a statistical decomposition, and its uncertainty could not be assessed with participant-level bootstrap resampling. Second, interpretation depends on the actual wording and scoring of the measures. General organizational ownership may differ from ownership of security resources, and opinion-expression measures developed for public issues may not capture security-specific silence. Constructive ownership should be distinguished from territoriality, and mixed-direction expression items require defensible aggregation. SeBIS covers selected personal practices rather than comprehensive organizational performance. Third, self-reports are vulnerable to recall error, social desirability, and common-method influences. Their magnitude cannot be determined from the correlation matrix, and neither low collinearity nor a one-factor test alone establishes the absence of method bias (Podsakoff et al., 2024).

Suggestions

Future research should use longitudinal designs to examine whether psychological ownership precedes changes in spiral of silence and information security behavior. Researchers should clearly identify the ownership target, distinguish constructive ownership from territoriality, and validate silence measures for workplace cybersecurity contexts. Self-report measures could be supplemented with behavioral assessments, while analyses should consider cybersecurity awareness, training, occupational roles, and organizational climate. More diverse samples across organizations and sectors would strengthen generalizability. Organizations should also evaluate initiatives that involve employees in security decisions, provide accessible channels for raising concerns, and encourage respectful managerial responses. Such initiatives should assess personal security practices and security-related communication separately to determine where improvements occur.

Implications

The theoretical contribution lies in considering the personal significance of organizational resources alongside the social inhibition of expression. Psychological ownership concerns why a target matters to an employee, while spiral-of-silence theory concerns when expression may be socially costly. Their integration offers a focused explanation to test for variation in protective practices. Establishing the indirect pathway requires evidence that the measures represent distinct constructs and that the association is sufficiently precise. The model should therefore guide stronger testing rather than be treated as an exhaustive explanation of employee cybersecurity.

For organizations, the findings suggest evaluating employee involvement in security decisions together with opportunities to seek clarification and raise concerns. Usable procedures, respectful managerial responses, and feedback following disclosures may help employees participate constructively. These practices should be assessed through appropriate intervention designs because the present associations do not demonstrate their effectiveness. Responsibility should be supported by resources, authority, and clear boundaries. A stronger sense of ownership should not justify bypassing access controls, withhold information, or treat a system as an employee's exclusive territory. Future research should specify the ownership target, separate constructive ownership from territoriality, and distinguish concealment, fear of isolation, and willingness to speak. Security-related adaptations require careful evaluation of their content and dimensional structure. Longitudinal designs can assess ordering, and privacy-preserving behavioral tasks or appropriately governed records can complement self-report outcomes.

V. CONCLUSION

Psychological ownership was positively associated with self-reported information security behavior and negatively associated with spiral of silence. Silence was negatively associated with security behavior after accounting for ownership and added information to the regression model. The indirect point estimate had the hypothesized direction. The findings support examining constructive ownership and communication reluctance together in behavioral cybersecurity.

Disclosure Statement
No potential conflict of interest was reported by the authors.

Funding
The author received no funding from any organizations.

VI.REFERENCES

Avey, J. B., Avolio, B. J., Crossley, C. D., & Luthans, F. (2009). Psychological ownership: Theoretical extensions, measurement and relation to work outcomes. *Journal of Organizational Behavior, 30*(2), 173–191. https://doi.org/10.1002/job.583

Bayram, A., & Bayer, N. (2019). Turkish adaptation of Spiral of Silence Scale: The study of reliability and validity. *Life Skills Journal of Psychology, 3*(6), 187–194. https://doi.org/10.31461/ybpd.610147

Bowen, F., & Blackmon, K. (2003). Spirals of silence: The dynamic effects of diversity on organizational voice. *Journal of Management Studies, 40*(6), 1393–1417. https://doi.org/10.1111/1467-6486.00385

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly, 43*(2), 525–554. https://doi.org/10.25300/MISQ/2019/15117

Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 2873–2882). Association for Computing Machinery. https://doi.org/10.1145/2702123.2702249

Hayes, A. F., & Coutts, J. J. (2020). Use omega rather than Cronbach's alpha for estimating reliability. But… *Communication Methods and Measures, 14*(1), 1–24. https://doi.org/10.1080/19312458.2020.1718629

Lee, H., Oshita, T., Oh, H. J., & Hove, T. (2014). When do people speak out? Integrating the spiral of silence and the situational theory of problem solving. *Journal of Public Relations Research, 26*(3), 185–199. https://doi.org/10.1080/1062726X.2013.864243

Marett, K., & Marett, E. G. (2026). Speaking up for security: The role of safety voice in improving organizational information security. *Organizational Cybersecurity Journal: Practice, Process & People*. Advance online publication. https://doi.org/10.1108/OCJ-08-2025-0033

Maxwell, S. E., & Cole, D. A. (2007). Bias in cross-sectional analyses of longitudinal mediation. *Psychological Methods, 12*(1), 23–44. https://doi.org/10.1037/1082-989X.12.1.23

Morrison, E. W. (2023). Employee voice and silence: Taking stock a decade later. *Annual Review of Organizational Psychology and Organizational Behavior, 10*, 79–107. https://doi.org/10.1146/annurev-orgpsych-120920-054654

Noelle-Neumann, E. (1974). The spiral of silence: A theory of public opinion. *Journal of Communication, 24*(2), 43–51. https://doi.org/10.1111/j.1460-2466.1974.tb00367.x

Petrič, G., & Orehek, Š. (2025). Expressing opinions about information security in an organization: The spiral of silence theory perspective. *Information & Computer Security, 33*(2), 223–241. https://doi.org/10.1108/ICS-04-2024-0083

Pierce, J. L., Kostova, T., & Dirks, K. T. (2001). Toward a theory of psychological ownership in organizations. *Academy of Management Review, 26*(2), 298–310. https://doi.org/10.5465/amr.2001.4378028

Podsakoff, P. M., Podsakoff, N. P., Williams, L. J., Huang, C., & Yang, J. (2024). Common method bias: It's bad, it's complex, it's widespread, and it's not easy to fix. *Annual Review of Organizational Psychology and Organizational Behavior, 11*, 17–61. https://doi.org/10.1146/annurev-orgpsych-110721-040030

Van Dyne, L., & Pierce, J. L. (2004). Psychological ownership and feelings of possession: Three field studies predicting employee attitudes and organizational citizenship behavior. *Journal of Organizational Behavior, 25*(4), 439–459. https://doi.org/10.1002/job.249

Verkijika, S. F. (2020). Employees' cybersecurity behaviour in the mobile context: The role of self-efficacy and psychological ownership. In *2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)* (pp. 1–5). IEEE. https://doi.org/10.1109/IMITEC50163.2020.9334097